PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-260640
(43)Date of publication of application : 16.09.2004

(51)Int.Cl. H04L 9/32

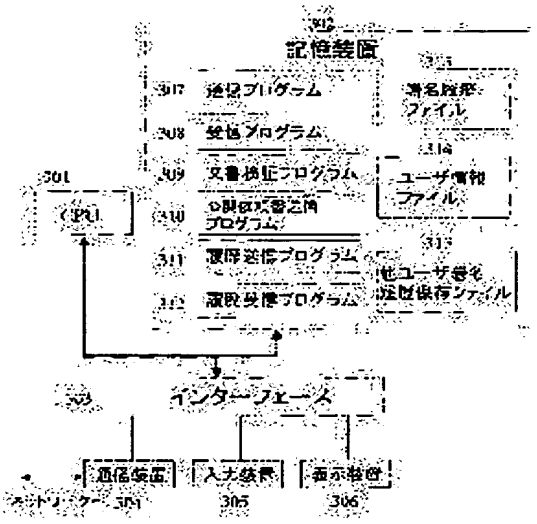
(21)Application number : 2003-050248
(22)Date of filing : 27.02.2003

(71)Applicant : HITACHI LTD
(72)Inventor : TANIMOTO KOICHI
MIYAZAKI KUNIHIKO
ITO SHINJI
KUDO YASUAKI
BESSHO RYOJI

(54) METHOD AND DEVICE FOR DISCLOSING SIGNATURE RECORD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a disclosure system which is for a public organization and is efficient and secure to the public organization and to provide a user with a signature verification function that uses a disclosed signature record.
SOLUTION: This public organization discloses a signature record received from a user to a Web. When the public organization opens the signature record, the public organization acquires a time stamp and returns the time stamp to the user as well as disclosure notification. The public organization has a signature history and periodically discloses a portion of the history to newspapers, etc. Otherwise, the public organization prepares data for disclosure on the basis of a signature record received from each user and discloses the data to the newspapers. The public organization transmits the signature history of the public organization to the user after disclosing the data to the newspapers.

図3



LEGAL STATUS

[Date of request for examination] 07.02.2006
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-260640
(P2004-260640A)
(43)公開日　平成16年9月16日(2004.9.16)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/32	H04L	9/00	675Z	5J104
	H04L	9/00	675B	

審査請求 未請求　請求項の数 14　OL　（全 21 頁）

(21)出願番号　特願2003-50248 (P2003-50248)
(22)出願日　平成15年2月27日 (2003.2.27)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１４年度通信・放送機構「次世代証拠基盤技術に関する研究開発」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

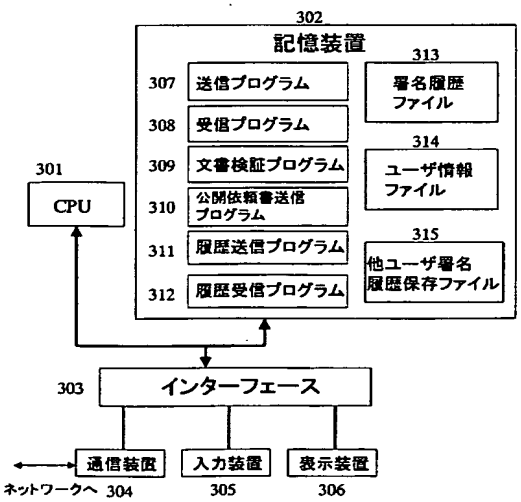
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　100075096
弁理士　作田　康夫
(72)発明者　谷本　幸一
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】署名記録の公開方法、および装置

(57)【要約】
【課題】公開機関のための、公開機関およびユーザにとって効率的で安全な公開システムと、ユーザに対して、公開された署名記録を利用した署名検証機能を提供する。
【解決手段】公開機関は、ユーザから受け取った署名記録をＷｅｂに公開する。公開時にはタイムスタンプを取得し、公開通知書とともにユーザに返信する。公開機関も署名履歴を持ち、履歴の一部を定期的に新聞等に公開する。もしくは、各ユーザから受け取った署名記録を基に公開用データを作成し、それを新聞に公開する。公開機関は、新聞公開後に公開機関の署名履歴をユーザに送信する。
【選択図】　図３

図３



【特許請求の範囲】
【請求項１】
ユーザ側装置が生成した署名に関わる情報を記録した署名記録の公開方法であって、
公開機関側装置において、
前記ユーザ側装置が作成したユーザ署名記録を受信し、公開するユーザ署名記録公開ステップと、
前記ユーザ署名記録を公開したことを、前記ユーザに通知するユーザ署名記録公開通知ステップと、
受信した前記ユーザ署名記録を用いた公開機関署名記録を作成し、過去に作成した公開機関署名記録が登録されている署名履歴を更新する署名履歴更新ステップと、
作成した前記公開機関署名記録を公開する公開機関署名記録公開ステップと、
前記公開機関署名記録を公開したことを前記ユーザに通知する公開機関署名記録公開通知ステップと、を有する
ことを特徴とする署名記録の公開方法。
【請求項２】
請求項１記載の署名記録の公開方法であって、
前記署名履歴更新ステップは、
前記公開機関署名記録を、受信した前記ユーザ署名記録と、複数の他の署名記録に基づいて作成し、署名履歴ファイルに記録する署名記録作成ステップと、
前記ユーザに関わる情報と受信した前記ユーザ署名記録に関する情報をユーザ情報ファイルに記録するユーザ情報ファイル更新ステップと、からなる
ことを特徴とする署名記録の公開方法。
【請求項３】
請求項１記載の署名記録の公開方法であって、
前記ユーザ署名記録公開ステップは、
前記ユーザ署名記録の公開日時を保証するタイムスタンプを取得するタイムスタンプ取得ステップを有する
ことを特徴とする署名記録の公開方法。
【請求項４】
請求項２記載の署名記録の公開方法であって、
前記署名記録作成ステップは、
前記ユーザ署名記録について、署名アルゴリズム識別情報と、署名記録固有に付けられる署名番号と、連鎖の検証に利用する前回署名記録のハッシュ値と、受信した前記ユーザ署名記録の署名番号とハッシュ値と、からなる前記公開機関署名記録を作成し、
前記署名履歴に新たに作成した前記公開機関署名記録を追加する
ことを特徴とする署名記録の公開方法。
【請求項５】
請求項２記載の署名記録の公開方法であって、
前記ユーザ情報ファイル更新ステップは、
前記公開機関署名記録に付けられた署名番号と、
対応する前記公開機関署名記録がユーザ署名記録の受信に応じて作られたことを示す受信符号と、
前記ユーザ署名記録の送信者を示す相手情報と、
受信したユーザ署名記録に付けられた署名番号と、
受信した前記ユーザ署名記録と、
からなるデータを作成して、前記ユーザ情報ファイルに追加する
ことを特徴とする署名記録の公開方法。
【請求項６】
請求項１記載の署名記録の公開方法であって、
前記公開機関側装置のユーザ署名記録公開通知ステップは、

公開したことを前記ユーザ側装置のユーザに通知するための公開通知書を作成する公開通知書作成ステップと、
作成した前記公開通知書と前記署名履歴中の前回署名記録から署名を作成し、前記公開通知書に添付する署名作成ステップと、
作成した署名の情報を前記署名履歴に記録する署名履歴更新ステップと、
前記ユーザに関わる情報を前記ユーザ情報ファイルに記録するユーザ情報ファイル更新ステップと、
作成した前記公開通知書を前記ユーザに送信する送信ステップと、からなる
ことを特徴とする署名記録の公開方法。

【請求項７】

請求項６記載の署名記録の公開方法であって、
前記公開通知書作成ステップは、
公開したことを前記ユーザに伝える文書と、
公開した公開署名記録と、
公開した日時を伝えるタイムスタンプと、
に基づいた公開通知書を作成する
ことを特徴とする署名記録の公開方法。

【請求項８】

請求項６記載の署名記録の公開方法であって、
前記署名履歴更新ステップは、
署名アルゴリズム識別情報と、
署名記録固有に付けられる署名番号と、
連鎖の検証に利用する前回署名記録のハッシュ値と、
署名作成対象文書のハッシュ値と、
作成した署名と、
とからなる署名記録を作成し、前記署名履歴に追加する
ことを特徴とする署名記録の公開方法。

【請求項９】

請求項６記載の署名記録の公開方法であって、
前記ユーザ情報ファイル更新ステップは、
署名記録と関連付けられた署名番号と、
対応する公開機関署名記録が署名作成時に作られたことを示す符号と、
前記公開通知書を送信する前記ユーザを示す相手情報と、
からなる情報を前記ユーザ情報ファイルに追加する
ことを特徴とする署名記録の公開方法。

【請求項１０】

請求項６記載の署名記録の公開方法であって、
前記公開機関署名記録公開ステップは、
前記公開通知書作成ステップに基づいて更新された署名履歴の一部を公開することを特徴とする署名記録の公開方法。

【請求項１１】

請求項２記載の署名記録の公開方法であって、
公開機関署名記録公開通知ステップは、
通知する前記ユーザを前記ユーザ情報ファイルから検索する送信相手検索ステップと、
送信すべき履歴を前記ユーザ情報ファイルから検索する送信履歴範囲取得ステップと、
前記公開機関署名記録を公開したことを通知する公開通知書作成ステップと、
作成した公開通知書と前回署名の署名記録から署名を作成する署名作成ステップと、
作成した署名の情報を前記署名履歴に記録する署名履歴更新ステップと、
通知する前記ユーザの情報を前記ユーザ情報ファイルに記録するユーザ情報ファイル更新ステップと、

作成した前記公開通知書を前記ユーザに送信する送信ステップと、を有する
ことを特徴とする署名記録の公開方法。
【請求項１２】
請求項１１記載の署名記録の公開方法であって、
前記公開通知書作成ステップは、
前記公開機関署名記録を公開したことを前記ユーザに伝える文書と、
公開した署名記録と、
送信する範囲の署名履歴と、
に基づいた公開通知書を作成する
ことを特徴とする署名記録の公開方法。
【請求項１３】
請求項１１記載の署名記録の公開方法であって、
前記ユーザ情報ファイル更新ステップは、
前記公開機関署名記録に付けられた署名番号と、
対応する前記公開機関署名記録が公開機関署名記録公開通知時に作られたことを示す符号と、
前記公開通知書を送信する前記ユーザを示す相手情報と、
送信する履歴の範囲を示す情報と、
とからなる情報を前記ユーザ情報ファイルに追加する
ことを特徴とする署名記録の公開方法。
【請求項１４】
請求項１記載の署名記録の公開方法であって、
前記ユーザ側装置は、当該ユーザ側装置において送信または受信したユーザ署名記録または公開機関署名記録の、送信または受信相手に関わる情報を記録するユーザ情報ファイルを備える
ことを特徴とする署名記録の公開方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ディジタル署名の証拠性を高める技術に関する。
【０００２】
【従来の技術】
ディジタル署名（以下、署名という）の証拠性を高める技術として、署名作成の際に、その時点までの署名履歴情報を反映させ、作成した署名に関わる情報は、署名記録として新たに署名履歴に追加する手法がある（例えば、特許文献１または特許文献２参照）。この方法により、作成した署名は連鎖構造を持つ。検証の際は、署名に対する検証の他に、連鎖の検証も行うことにより、改竄は困難となる。
【０００３】
この手法においては、連鎖が繋がっている署名は正当なものであると判断するが、その正当性を確実に証明するためには、署名履歴中に信頼できる正当な署名記録があることが望ましい。この信頼できる署名記録を作り出すために、上記手法では、解決策の一つとして、署名記録の定期的な公開が挙げられている。
【０００４】
上記手法を用いて署名を作成する各ユーザは、定期的もしくは定数回毎に最新の署名記録を公開する。署名記録を例えば、新聞や官報などの刊行物（以下、新聞という）に公開することにより、正当な署名作成者以外が作成した不正な署名記録は、正当な署名作成者の指摘により発覚するため、公開した署名記録は、正当な署名記録であるものとして扱うことができる。また、一般に公開されるため、公開した署名記録は、後から取り消したり、改竄したりすることは困難である。
【０００５】

【特許文献１】
特開２００１－３３１１０４号公報
【特許文献２】
特開２００１－３３１１０５号公報
【０００６】
【発明が解決しようとする課題】
上記技術において、ユーザの数が多い場合、各ユーザの署名記録を全て新聞に公開することは現実的に難しい。従って、より実用的な仕組みが望まれる。
【０００７】
【課題を解決するための手段】
本発明は、各ユーザが個別に新聞公開するのではなく、その新聞公開をまとめて代行する公開機関を設ける。
【０００８】
すなわち、本発明は、公開機関側装置およびユーザ側装置のための効率的で安全な公開システムと、ユーザに対して、公開された署名記録を利用した署名検証機能を提供する。
【０００９】
本発明において、「署名記録」とは、作成あるいは受信した個々の署名の生成に関わる情報であり、「署名履歴」とは、複数の「署名記録」が保存されたファイルを指す。
【００１０】
本発明の公開システムでは、ユーザ側装置は、署名作成時に他の署名記録から得られる情報を反映させる署名技術（以下、ヒステリシス署名という）を利用し、作成した署名記録を署名履歴に追加する。さらに作成した署名記録を、公開依頼書に添付して公開機関に送信して公開を依頼する。
【００１１】
公開機関側装置は、各ユーザ側装置から公開依頼書に添付されたユーザ署名記録（以下、公開署名記録という）を受信し、Ｗｅｂなどを利用して第３者がアクセス可能なように公開する。これにより、各ユーザは、各々が署名記録を新聞公開したのと同等の信頼性を得ることができるので、自身の署名履歴中に信頼できるポイントを作ることができる。また、各ユーザは公開された署名記録を任意の時間に任意の場所で取得することができる。取得した署名記録は、正当な署名記録として連鎖検証の起点に利用される。
【００１２】
また、公開機関側装置は、各ユーザから送られてきた公開署名記録を公開機関が管理するＷｅｂ等に公開した際には、それぞれのユーザに対して署名付きのＷｅｂ公開通知書を送付する。これによりユーザは、自分の公開署名記録が確実に公開機関によって公開されたことを知ることができる。正規のユーザ側に、公開依頼した覚えが無いのにＷｅｂ公開通知書が届いた場合は、他人のなりすましによって不正に公開されたことになる。
【００１３】
また、公開機関側装置は、公開時にタイムスタンプを取得し、Ｗｅｂ公開通知書にこのタイムスタンプを添付してもよい。このタイムスタンプにより、Ｗｅｂ公開通知書を受け取ったユーザは、公開日時を確認することができる。また、タイムスタンプの添付されたＷｅｂ公開通知書に公開機関の署名が付けられた場合、公開した署名記録の内容と公開日時が保証され、このＷｅｂ公開通知書の情報を用いることにより、ユーザの署名履歴中に日時の確定した署名記録を作ることができる。すなわち、その署名記録以前（以後）に作られた署名は、Ｗｅｂ公開通知書に記載の日時以前（以後）に作られたものであることを証明することができる。
【００１４】
公開機関自身も公開機関の署名履歴を持ち、公開機関側装置は、ユーザ側装置から公開署名記録を受信した時、署名の検証を行うとともに、受信した公開署名記録を含んだ公開機関の署名記録を作成し、公開機関の署名履歴を更新する。また、公開機関側装置は、ユーザ側装置へのＷｅｂ公開通知書送信の時には、署名の作成を行うとともに、公開機関の署

名履歴を更新する。公開機関側装置において、各ユーザ側装置から受け取った公開署名記録を含んだ署名記録を公開機関の署名履歴に追加することにより、公開機関あるいはユーザが公開機関の署名履歴の連鎖を調べることによって、公開後の公開署名記録の改竄を検知できるようになる。また、公開機関側装置は、ユーザ側装置から公開署名記録を受信した時や、ユーザへＷｅｂ公開通知書を送信した時には、署名履歴の更新とともに公開機関のユーザ情報ファイル（ユーザ情報を保存したファイル）も更新する。ユーザ情報ファイルは、Ｗｅｂ公開通知書の送付や署名履歴の送信の際に、送信先や送信する署名履歴の範囲を確定するために参照される。

【００１５】

また、公開機関側装置は、公開署名記録を公開機関に送信したユーザに対して、そのユーザから公開署名記録を受信した時点から、その後最初に新聞公開した時点の間に作られた公開機関の署名履歴を送信する。これによりユーザ側装置は、署名検証（連鎖検証を含む）の際に、この送信された署名履歴を利用して、公開機関が新聞に公開した署名記録から公開機関の署名履歴の連鎖をたどって署名検証を行うことができる。

【００１６】

また、公開機関側装置は、適当な時期に、または定期的に（例えば、毎週１回）、新聞に公開機関の署名履歴中の署名記録を公開する。また、公開機関側装置は、各ユーザ側装置から送られてきた公開署名記録を用いて新聞公開用データを作成し、それを公開してもよい。公開された署名記録あるいは新聞公開用データを用いて署名検証を行うことにより、公開機関の署名履歴の正当性を保証し、公開機関自身の公平性を示すことができる。

【００１７】

本発明によれば、公開機関がユーザ側装置の署名記録の公開を代行することにより、より多くのユーザが自身の署名の正当性を証明できるようになる。

【００１８】

【発明の実施の形態】

図１は、本発明を適用した一実施形態における公開システムの概略図である。

【００１９】

図示するように、本公開システムは、署名記録の公開を依頼し、公開機関から受け取った署名履歴を利用して署名を検証するユーザ側装置１０１～１０３と、各ユーザから送られてきた署名記録を公開、また自身の署名記録もしくは正当性を示す署名履歴を公開、署名の検証に必要な署名履歴を各ユーザに送信する公開機関側装置１０４とを含んで構成される。ユーザ側装置１０１～１０３と公開機関側装置１０４は、ネットワーク１０５を介して繋がっている。

【００２０】

公開機関側装置１０４は、図２に示すように、記憶装置２０２と、ネットワークを介して他の装置と通信を行うための通信装置２０４と、通信装置２０４を介して繋がるＷｅｂサーバ２０７と、キーボードやマウスなどの入力装置２０５と、ディスプレイなどの表示装置２０６と、ＣＰＵ２０１とから構築することができる。

【００２１】

記憶装置２０２には、公開システムの機能を実現するプログラム（公開依頼書受信プログラム２０８、公開通知書送信プログラム２０９、新聞公開プログラム２１０、履歴送信プログラム２１１、ユーザ管理プログラム２１２）と、署名履歴ファイル（署名履歴ともいう）２１３と、ユーザ情報ファイル２１４と、各ユーザから受信した署名記録等が保存されている公開署名記録保存ファイル２１５が格納されている。プログラム２０８～２１２は、ＣＰＵ２０１により実行され、署名の作成や検証、ユーザから受信した署名記録の保存とＷｅｂ公開、公開機関自身の署名記録の新聞公開、公開機関の署名履歴の読込や更新、公開機関のユーザ情報ファイルの読込や更新を行う機能を、公開機関側装置上に具現化する。

【００２２】

各プログラムは、予め記憶装置２０２に格納されていてもよいし、公開機関側装置が利用

可能な媒体を介して導入されてもよい。媒体とは、たとえば、公開機関側装置に着脱可能な記憶媒体や、通信装置２０４に接続するネットワークまたはネットワークを伝搬する搬送波といった通信媒体を含む。

【００２３】

ユーザ側装置は、図３に示すように、記憶装置３０２と、ネットワークを介して他の装置と通信を行うための通信装置３０４と、キーボードやマウスなどの入力装置３０５と、ディスプレイなどの表示装置３０６と、ＣＰＵ３０１とから構成される。

【００２４】

記憶装置３０２には、署名を作成して署名付き文書を送信する送信プログラム３０７と署名付き文書を受信して署名を検証する受信プログラム３０８と署名履歴の連鎖検証も含んだ検証を行う文書検証プログラム３０９と公開依頼書を作成して公開書名記録を公開機関に送信する公開依頼書送信プログラム３１０と自分の署名履歴を他のユーザに送信する履歴送信プログラム３１１と他のユーザから他のユーザの署名履歴を受信する履歴受信プログラム３１２と署名履歴ファイル（署名履歴という）３１３とユーザ情報ファイル３１４と他ユーザから受信した署名履歴を保存するファイル３１５が格納されている。プログラム３０７～３１２は、ＣＰＵ３０１により実行され、署名の作成や検証、署名履歴の読込や更新、ユーザ情報ファイルの読込や更新を行う機能を、ユーザ側装置１０１～１０３上に具現化する。

【００２５】

ユーザ側装置１０１～１０３は、署名作成時に署名履歴情報を反映させるヒステリシス署名技術を利用している。

【００２６】

図４は、ユーザ側装置１０１～１０３が、ヒステリシス署名技術に基いて、送信文書４０７に対し署名を作成した後、署名付き受信文書４０９を受信し署名検証した場合の署名履歴の様子を示したものである。

【００２７】

署名作成時には、送信文書４０７と前回の署名記録４１３のハッシュ値に対して秘密鍵を作用させて署名４０８を作成する。作成後、前回の署名記録４１３と作成した署名４０８から、署名記録４１４を作成し、署名履歴３１３に追加する。どの署名がどの署名記録中に残っているか判別するために、署名作成時においては、署名履歴に今回新たに追加される署名記録の署名番号を、作成した署名に付加する。作成された署名記録が順に記録されたファイルが署名履歴３１３である。

【００２８】

署名受信時には、受信文書４０９に対する署名４１０を公開鍵を用いて検証する。検証後、前回の署名記録４１４のハッシュ値と署名４１０から署名記録４１５を作成し、署名履歴４１１に追加する。以上のように、署名作成時や署名受信時において、署名情報を記録した署名記録が作られる。前回の署名情報が次回の署名作成に利用されるため、署名間に連鎖関係が生じる。通常の公開鍵を用いた署名検証に加えて、この連鎖関係を検証することにより、より確実な署名の検証を行うことができる。

【００２９】

ユーザ側装置１０１～１０３における署名記録４１２～４１５は、署名アルゴリズム等の情報を示す「識別番号４０１」、何番目に作られた署名記録であるかを示す「署名番号４０２」、署名作成（送信）時に作成した署名記録か、署名検証（受信）時に作成した署名記録かを表す「種別４０３」、連鎖検証に利用する「前回署名記録のハッシュ値４０４」、署名作成時のみ記録する「署名作成対象文書のハッシュ値（文書のハッシュ値という）４０５」、「署名ｏｒ受信署名記録情報４０６」（署名作成時は、作成した署名。署名検証時は、受信した署名の署名番号とその署名に対する署名記録のハッシュ値を結合したもの）から成る。

【００３０】

図５にユーザと公開機関の間でやり取りされるデータの流れを図示する。

【００３１】
ユーザ側装置１０１～１０３は、適当な時期あるいは定期的に、公開したい署名記録（たとえばその時点での最新の署名記録）を添付した公開依頼書５０６を公開機関側装置１０４に送信する（５０１）。これにより、ユーザの署名履歴３１３中に信頼性を保証された署名記録を作ることが可能となる。この公開機関に送信した署名記録は、公開署名記録という。

【００３２】
ユーザ側装置１０１～１０３より公開署名記録を受け取った公開機関側装置は、その公開署名記録を自身の記憶装置２０２に保管するとともに、Ｗｅｂなどを利用して公開する（５０２）。公開後に、公開した公開署名記録の作成者であるユーザに対して、公開した旨を知らせるＷｅｂ公開通知書５０７を送信する（５０３）。

【００３３】
公開機関は、適当な時期、あるいは定期的に新聞に自身の署名記録を公開（公開した署名記録を以降、新聞公開署名記録と呼ぶ）する（５０４）。新聞公開後に、前回の新聞公開時点から今回の新聞公開時点までの間に、ステップ５０２で公開された公開署名記録の公開を依頼したユーザに対して、新聞公開した旨を知らせる新聞公開通知書５０８を送信する（５０５）。新聞公開通知書には、ユーザが新聞公開署名記録を利用して署名の検証が行えるような情報を添付する。

【００３４】
本実施例においては、公開機関側装置１０４も、署名作成時に署名履歴情報を反映させる上記ヒステリシス署名技術を利用する。図６は、公開システムの機能を実現するための、公開機関側装置１０４の署名履歴２１３とユーザ情報ファイル２１４の構成の一例である。

【００３５】
公開機関側装置１０４の署名履歴ファイル２１３は、公開機関側装置で作成された署名記録が順に記録されたファイルであり、各レコード６０１～６０３は、識別番号６０４、署名番号６０５、種別６０６、前回署名記録のハッシュ値６０７、公開機関側装置で作成する署名の対象となる文書のハッシュ値（文書のハッシュ値という）６０８、署名ｏｒ受信した公開署名記録情報６０９（署名作成時は、作成した署名。署名検証時は、受信した公開署名記録の署名番号と公開署名記録のハッシュ値を結合したもの）からなる。

【００３６】
「識別番号６０４」は、公開機関側装置１０４が利用している署名アルゴリズム等の情報を示す番号であり、これによって、署名記録６０１～６０３が作成された時に、どの種類の暗号やハッシュ関数が使われたのかを判別する。

【００３７】
「署名番号６０５」は、連番で付与され、署名履歴の中から特定のレコード（署名記録）を指定するのに用いられる。どの署名がどの署名記録中に残っているか判別するために、署名作成時においては、署名履歴に今回新たに追加される署名記録の「署名番号６０５」を、作成した署名に付加する。

【００３８】
「種別６０６」は、署名記録６０１～６０３が署名作成（送信）時に作成されたものか、署名検証（受信）時に作成されたものかを示す符号であり、例えば、署名記録６０１は、種別６０６の値により、署名検証（受信）時に作成されたものであると分かる。

【００３９】
「前回署名記録のハッシュ値６０７」は、署名履歴の連鎖検証に用いられるものであり、例えば、署名番号「２」で指定される署名記録６０２における「前回署名記録のハッシュ値６０７」の「Ｈ（Ｓ１）」は、署名記録６０１における各項目６０４～６０９の各値からなるデータＳ１（Ｓ１はたとえば各値を結合する）のハッシュ値（ハッシュ関数をＨ（ｘ）とする）である。

【００４０】

「文書のハッシュ値６０８」を署名履歴２１３の項目のひとつに含めてもよい。この項目を用いることによって、改竄するためには、それに対応する署名の作成対象となった文書が必要となるため、改竄がより困難になる。

【００４１】

「署名ｏｒ受信した公開署名記録情報６０９」には、公開機関装置での署名作成（送信）時には、作成した署名を登録する。例えば、署名記録６０２においては、署名番号「２」、前回署名記録のハッシュ値「Ｈ（Ｓ１）」、文書のハッシュ値６０８「Ｈ（Ｍ２）」からなるデータに対する署名「Ｓｉｇｎ（２‖Ｈ（Ｓ１）‖Ｈ（Ｍ２））」を登録する。また、公開依頼書５０６を受信した時には、添付されていた公開署名記録の署名番号とハッシュ値とからなるデータを登録する。例えば、署名記録６０３においては、「署名ｏｒ受信した公開署名記録情報６０９」には、受信した公開依頼書５０６に添付された公開署名記録の署名番号が「１５」で、公開署名記録のハッシュ値が「Ｈ（Ｓ１５）」であれば、これらを結合した「１５‖Ｈ（Ｓ１５）」を登録する。

【００４２】

ユーザ情報ファイル２１４は、公開機関側装置での取引記録が順に記録されたファイルであり、各レコード６１０～６１６は、署名番号６１７、種別６１８、取引相手の情報（相手情報という）６１９、受信した署名の署名番号（受信署名番号という）６２０、公開署名記録６２１、タイムスタンプの日時（日時という）６２２からなる。

【００４３】

「署名番号６１７」には、何番の署名記録が誰と署名を取引した時に作成されたものであるかが分かるように、署名記録の署名番号６０５と対応した番号が登録する。

【００４４】

「種別６１８」は、６１０～６１６の各レコード（取引記録）が署名作成（送信）時に作成されたものであるか、署名検証（受信）時に作成されたものであるか、新聞公開時５０４に作成されたものであるか、新聞公開通知書送信（署名履歴送信）時５０５に作成されたものであるかを示す符号である。例えば、署名番号「３」で指定されるレコード６１３は、項目６１８の値により、署名検証（受信）時に作成されたものであると分かる。

【００４５】

「相手情報６１９」には、署名付き文書の送信相手や公開依頼書５０６の送信元などの情報（例えば、メールアドレス）を登録する。例えば、署名番号「３」で指定されるレコード６１３は、項目６１９の値により、ユーザＢとの取引情報を示すものであることが分かる。

【００４６】

「受信した署名の署名番号（受信署名番号という）６２０」には、受信した公開依頼書などの署名付き文書に付けられていた署名の署名番号を登録する。例えば、署名番号「３」で指定されるレコード６１３は、項目６２０の値により、「１６」の署名番号の署名が付いた署名付き文書を受信した時に作成されたものである。

【００４７】

「公開署名記録６２１」には、公開署名記録が添付された公開依頼書５０６を受信した時に、その添付されていた公開署名記録を登録する。例えば、署名番号「３」で指定されるレコード６１３は、項目６２１の値により、公開署名記録「Ｓ１５」が添付された公開依頼書を受信した時に作成されたものである。

【００４８】

「日時６２２」には、公開依頼書に添付された公開署名記録を受信した（５０２）時の日時、あるいは、公開機関の署名記録を新聞公開した（５０４）時の日付を登録する。

【００４９】

「署名番号６１７」により、例えば、署名履歴２１３の署名番号「３」で指定されるレコード６０３とユーザ情報ファイル２１４の署名番号「３」で指定されるレコード６１３とは対応していることが分かり、署名記録６０３は、取引記録６１３の各値により、ユーザＢから公開依頼書を受信した時に作成されたものであり、公開依頼書には、署名番号「１

６」の署名と、公開署名記録「Ｓ１５」が添付されており、この公開署名記録「Ｓ１５」は、「２００２年１０月１９日１５時５０分」に公開機関側装置が受信したものであると分かる。

【００５０】

ユーザ側装置１０１～１０３も、ユーザ情報ファイル３１４を持つ。ユーザ情報ファイル３１４は、他のユーザとの取引情報、公開機関との取引情報を調べるのに利用される。ユーザ側装置のユーザ情報ファイル３１４は公開機関側装置のユーザ情報ファイル２１４とは異なり、ユーザ側装置のユーザ情報ファイルには項目６２０「公開署名記録」、項目６２１「日時」に該当する部分は無い。ユーザ側装置のユーザ情報ファイル３１４は、何番の署名記録は誰と取引した署名のものであるかが分かるように、署名記録の署名番号と対応する「署名番号」、対応する署名記録が、署名作成（送信）時に作られたか、署名検証（受信）時に作られたか、公開機関に公開した時に作られたかを表す「種別」、「取引相手の情報（相手情報という）」、「受信した署名の署名番号（受信署名番号という）」で構成する。

【００５１】

公開機関側装置は、公開システムの公開依頼書受信プログラム２０８を用いて、ユーザから送信されてきた公開署名記録が添付された署名付き公開依頼書５０６を受信する。

【００５２】

図７にユーザによる公開依頼書送信プログラム３１０と公開機関の公開依頼書受信プログラム２０８のフロー図を示す。

【００５３】

ユーザ側装置１０１～１０３において、Ｓ７０１で、公開したい情報（公開署名記録）を取得し、それを添付した公開依頼書５０６を作成する。Ｓ７０２で、Ｓ７０１で作成した公開依頼書に対して署名を作成し、Ｓ７０３で署名付き公開依頼書を公開機関側装置に送信する。

【００５４】

公開依頼書を受信した公開機関側装置において、Ｓ７０４で、まずユーザが公開機関に登録されているか、すなわちユーザが正規の公開機関利用者であるかどうかを、例えば登録データベース（公開機関を利用希望するユーザを登録したリスト）を用いて確認し、公開依頼書に署名が付けられている場合は、Ｓ７０５で、送信元ユーザの公開鍵を用いて署名を検証する。公開鍵は、公開鍵証明書とともに署名付き公開依頼書に添付されていればその公開鍵を利用し、あるいは公開鍵証明書発行元より取得すればよい。

【００５５】

署名検証後、Ｓ７０６で、受信したユーザの公開署名記録を用いて、「識別番号６０４」、「署名番号６０５」、「前回署名記録のハッシュ値６０７」、「受信した公開署名記録情報６０９」を、たとえば結合して作成した署名記録を作成し、署名履歴２１３に追加する。

【００５６】

Ｓ７０７で、タイムスタンプを取得し、Ｓ７０８で、ユーザ情報ファイルに、Ｓ７０６で作成した署名記録の「署名番号６１７」、公開依頼書を受信したことを示す「受信符号６１８」、公開依頼書を送信した送信元のユーザ情報である「相手情報６１９」、「受信した署名の署名番号（公開依頼書にＳ７０２によって署名が付けられていた場合）６２０」、受信した「公開署名記録６２０」、取得したタイムスタンプを用いた「日時６２１」を記録する。タイムスタンプは、例えばタイムスタンプ発行機関から取得すれば良い。また、上記送信元のユーザ情報としては、例えばメールアドレスを登録すればよい。

【００５７】

図７のＳ７０３において、ユーザＡから署名番号３１の公開署名記録Ｓ３１が添付された公開依頼書が公開機関に送信された場合には、Ｓ７０６によって、署名履歴２１３の各項目６０４～６０９の値「Ｖｅｒ．１．０（公開機関が利用する署名アルゴリズム等の情報を示す値）」、「１」、「受信」、「Ｈ（Ｓ０）（前回の署名記録のハッシュ値）」、「

ー（受信時なので、文書のハッシュ値は無し）」、「３１‖Ｈ（Ｓ３１）」が結合したレコード６０１が新たに記録される。

【００５８】

Ｓ７０８によって、ユーザ情報ファイル２１４の各項目６１７～６２２の値「１」、「受信」、「ユーザＡ@ＸＸＸ．ｃｏ．ｊｐ（ユーザＡのメールアドレス）」、「３２（Ｓ７０２によって公開依頼書に付けられた署名の署名番号）」、「Ｓ３１」、「２００２．１０．１７．０８１６（公開依頼書を受信した日時）」が結合したレコード６１１が新たに記録される。

【００５９】

Ｓ７０９で、Ｗｅｂ上に公開依頼書送信元のユーザ名と公開依頼書に添付された公開署名記録を公開する。

【００６０】

公開機関側装置１０４は、公開依頼書受信プログラム２０８により、ユーザから受信した公開署名記録をＷｅｂに公開（５０２）した後、Ｗｅｂ公開通知書送信プログラム２０９により、その公開署名記録の送信元のユーザにＷｅｂに公開した旨を伝えるＷｅｂ公開通知書５０７を送信する。

【００６１】

公開機関側装置１０４の公開通知書送信プログラム２０９の処理フローについて、図８を用いて説明する。

【００６２】

Ｓ８０１で、公開依頼書を送信してきたユーザに対してＷｅｂに公開した旨を伝えるＷｅｂ公開通知書５０７を作成する。Ｗｅｂ公開通知書には、上記公開依頼書を送信してきたユーザから依頼されて公開した公開署名記録（公開依頼書に添付されていた署名記録）やＳ７０７により取得したタイムスタンプなどを添付しても良い。添付した場合には、公開機関がそのＷｅｂ公開通知書に署名をつけると、Ｗｅｂ公開通知書を受け取ったユーザは公開署名記録がいつ公開されたかを証明することができ、少なくともその日時以前にその署名記録が存在していたことを示すことができる。

【００６３】

Ｓ８０２で、新たな署名番号（前回作成した署名記録の署名番号に１足したもの）と前回署名記録のハッシュ値とＳ８０１で作成したＷｅｂ公開通知書のハッシュ値からなるデータをたとえば結合により作成して、それに対して署名を作成する。例えば、署名履歴２１３にレコード６０１が記録された状態で、公開通知書送信プログラム２０９によりユーザＡにＷｅｂ公開通知書を送信する時には、署名番号６０５の「１」に１を足した値「２」と前回署名記録６０１のハッシュ値６０７「Ｈ（Ｓ１）」と文書のハッシュ値（ここではＷｅｂ公開通知書のハッシュ値）６０８「Ｈ（Ｍ２）」から、署名「Ｓｉｇｎ（２‖Ｈ（Ｓ１）‖Ｈ（Ｍ２））」を作成する。

【００６４】

Ｓ８０３で、Ｓ８０２で作成した署名に関する情報を署名記録として、署名履歴２１３に追加する。この時の署名記録は、上記例の場合は、識別番号６０４「Ｖｅｒ．１．０（公開機関が利用する署名アルゴリズム等の情報を示す値）」、署名番号６０５「２」、種別６０６「送信」、前回署名記録のハッシュ値６０７「Ｈ（Ｓ１）」、文書のハッシュ値６０８「Ｈ（Ｍ２）（Ｗｅｂ公開通知書のハッシュ値）」、署名６０９「Ｓｉｇｎ（２‖Ｈ（Ｓ１）‖Ｈ（Ｍ２））」から、たとえば結合により作成する。作成したレコード６０２が署名履歴２１３に新たに記録される。

【００６５】

Ｓ８０４で、ユーザ情報ファイル２１４に、「署名番号６１７」、「種別６１８」、「相手情報６１９」を記録する。上記例の場合は、各々、Ｓ８０３で作成した署名記録の署名番号「２」、Ｗｅｂ公開通知書を送信したことを示す送信符号「送信」、Ｗｅｂ公開通知書の送信先のユーザ情報（例えば、メールアドレス）「ユーザＡ@ＸＸＸ．ｃｏ．ｊｐ（Ｗｅｂ公開通知書の送信先のユーザＡのメールアドレス）」が結合されたレコード６１２

がユーザ情報ファイル２１４に新たに記録される。

【００６６】

Ｓ８０５で、Ｓ８０２で作成した署名の付いたＷｅｂ公開通知書をユーザに送信する。

【００６７】

図５に示すように、公開機関は、適当な時期に、または定期的に公開機関の署名履歴中の最新の署名記録を新聞などに公開する（５０４）。これによって、公開機関の署名履歴中に、公開後は変更不可能な署名記録、すなわち信頼できる署名記録を作り出すことができる。公開機関の署名履歴中に信頼できる署名記録を作り出すことによって、公開機関自体の不正を防ぎ、ユーザから、より大きな信用を得る。

【００６８】

新聞公開した信頼できる署名記録から連鎖が辿れる署名履歴は正当なものであり、ユーザは、新聞等に公開した公開機関の署名記録、公開機関の署名履歴、各ユーザの公開署名記録、各ユーザの署名履歴を用いて、署名を検証することができる。

【００６９】

公開機関側装置１０４の新聞公開プログラム２１０の処理フローを図９を用いて説明する。

【００７０】

Ｓ９０１で、新聞公開するデータを取得する。具体的には、署名履歴２１３中、最新の署名記録を取得する。例えば、署名履歴２１３にレコード６０１～６０３が記録されている状態であるとすると、署名記録６０３が新聞公開の対象となる（新聞公開署名記録と呼ぶ）。

【００７１】

Ｓ９０２で、今回作成する署名の署名番号（前回作成した署名記録の署名番号に１足したもの）と前回署名記録のハッシュ値と新聞公開署名記録のハッシュ値とからなるデータをたとえば結合により作成し、それに対して署名を作成する。

【００７２】

Ｓ９０３で、Ｓ９０２で作成した署名に関する情報を署名記録として、署名履歴２１３に追加する。署名記録は、「識別番号６０４」、「署名番号６０５（今回作成した署名の署名番号）」、「前回署名記録のハッシュ値６０７」、「文書のハッシュ値６０８（新聞公開署名記録のハッシュ値）」、「署名６０９（Ｓ９０２で作成した署名）」を結合したものである。

【００７３】

Ｓ９０４で、Ｓ９０３で作成した署名記録の「署名番号６１７」、「種別６１８」、「相手情報６１９」、「公開署名記録６２１」、「日時６２２」をユーザ情報ファイル２１４に記録する。上記例の場合は、例えば、各々、「新聞公開したことを示す新聞公開符号」「公開先の情報（公開先名）」「新聞公開署名記録」「公開日時」がレコード６１５に記録される。

【００７４】

Ｓ９０５で、新聞公開署名記録を新聞に公開する。このとき、公開機関の署名をつけて公開しても良いし、新聞公開署名記録のハッシュ値を公開しても良い。

【００７５】

公開機関は、新聞公開を行った後、前回の新聞公開から今回の新聞公開までの期間で受信した公開署名記録について、その送信元のユーザに、履歴送信プログラム２１１を用いて、公開機関の署名履歴を送信する。これにより、公開機関だけではなく各ユーザの手元にも、公開機関の新聞公開署名記録からユーザの署名履歴まで連鎖を遡って検証できる情報を残すことができる。例えば、１０年後に万一、公開機関が無くなってしまっても、各ユーザの手で検証が可能となる。

【００７６】

履歴送信プログラム２１１の処理フローについて図６と図１０を用いて説明する。

【００７７】

Ｓ１００１では、署名履歴を送信する相手を公開機関のユーザ情報ファイル２１４から検索する。検索の際には、最新の新聞公開署名記録を新聞公開した時点から、前回新聞公開署名記録を新聞公開した時点までの間で、公開機関がＷｅｂ公開通知書を送信した送信先のユーザを特定する。具体的には、種別６１８に新聞公開したことを示す符号が付いている最新の取引記録（レコード）とそれ以前で最新の新聞公開符号が付いている取引記録との間の取引記録を調べ、種別６１８に送信符号が付いている取引記録を探す。その取引記録の相手情報６１９が、署名履歴を送信する相手に関する情報である。

【００７８】

例えば、ユーザ情報ファイル２１４において、種別６１８を見てみると、「新聞」により、レコード６１５が最新の新聞公開した時の取引記録であり、レコード６１０が前回新聞公開した時の取引記録であることが分かる。それらの間のレコード６１１～６１４の種別６１８に「送信」が登録されているレコードは、６１２と６１４である。レコード６１２と６１４の相手情報６１９により、署名履歴を送信すべき相手は、ユーザＡとユーザＢであることが分かる。

【００７９】

Ｓ１００２で、ユーザ情報ファイル２１４を利用して、Ｓ１００１で特定した送信先に、どの範囲の署名履歴を送信すればよいか求める。まず（１）Ｓ１００１で特定した署名履歴送信先が記録されていた取引記録の署名番号を調べ、（２）次に最新の新聞公開した署名記録の署名番号を調べる。（１）の署名番号から（２）の署名番号までが送信する履歴の範囲である。例えば、Ｓ１００１において、レコード６１２によりユーザＡが署名履歴の送信先として特定されたとすると、レコード６１２の項目６１７の値が１であり、レコード６１５の署名番号６１７の値が５であるから、署名番号６１７の値が１～５の署名履歴が、ユーザＡに送信すべき履歴の範囲である。

【００８０】

Ｓ１００３では、Ｓ１００２で決定した範囲の署名履歴を添付した新聞公開通知書５０８を作成し、

Ｓ１００４で、今回作成する署名の署名番号（前回作成した署名記録の署名番号に１足したもの）と前回署名記録のハッシュ値と新聞公開通知書のハッシュ値とからなるデータに対して署名を作成する。

【００８１】

Ｓ１００５で、Ｓ１００４で作成した署名に関する情報を署名記録として、署名履歴２１３に追加する。署名記録は、識別番号６０４、署名番号６０５、前回署名記録のハッシュ値６０７、文書のハッシュ値（ここでは、新聞公開通知書のハッシュ値）６０８、署名６０９（Ｓ１００３で作成した署名）を結合したものである。

【００８２】

Ｓ１００６で、ユーザ情報ファイル２１４の、例えばレコード６１６のように、署名番号６１７、種別６１８、相手情報６１９にそれぞれ、Ｓ１００５で作成した署名記録の署名番号、新聞公開通知書を送信したことを示す履歴送信符号、新聞公開通知書の送信先のユーザ情報（例えば、メールアドレス）を記録する。

【００８３】

Ｓ１００７で、Ｓ１００４で作成した署名付き新聞公開通知書をユーザに送信する。

【００８４】

公開機関側装置１０４では、公開機関を利用するユーザおよび、ユーザから受信した公開署名記録をユーザ管理プログラム２１２によって管理する。公開機関側装置ではユーザ管理プログラム２１２を用いて、自身のデータベースに公開機関を利用するユーザを登録する。また、ユーザの要望、もしくは公開機関の判断で、ユーザ情報の追加・更新、ユーザの削除を行ってもよい。

【００８５】

ユーザが公開機関に公開署名記録の公開を依頼し、公開機関側装置が公開依頼書受信プログラム２０８によってユーザの公開署名記録を公開し、新聞公開プログラム２１０によっ

て署名履歴２１３中の署名記録を新聞公開することにより、ユーザは、自分の署名履歴中に新聞公開したのと同等の信頼性を持つ署名記録を持つことができる。

【００８６】

図１１を用いて、検証に利用できるユーザの署名履歴や公開機関の署名履歴を持つユーザ側装置の文書検証プログラム３０９が検証対象文書の署名を検証する場合を例にあげて説明する。

【００８７】

図１１において、ユーザが署名番号２の署名が添付された文書１２１０を検証する場合、Ｓ１２０１で、文書と署名に対して公開鍵を用いた通常の署名検証を行い、Ｓ１２０２で、検証に利用するユーザ側装置の署名履歴３１３中の署名番号２の署名記録の項目６０９に、検証対象のＮｏ．２の署名が残っているかどうか検証する。

【００８８】

Ｓ１２０３で、署名履歴３１３中Ｎｏ．２以降でＮｏ．２に一番近い公開署名記録を検索する（本例では、Ｎｏ．７がそれに該当する署名記録とする）。公開依頼書に添付する公開署名記録は、それまでの最新の署名記録であるので、Ｎｏ．８の署名記録が公開機関に公開依頼書を送信した時に作成されたとすると、この時公開された公開署名記録は、Ｎｏ．７の署名記録であることが、ユーザ情報ファイル３１４よりわかる。従って、Ｎｏ．２以降でＮｏ．２に一番近い公開署名記録は、Ｎｏ．７の署名記録である。ただし、Ｎｏ．２以降であれば、必ずしも一番近い公開署名記録でなくてもよい。

【００８９】

Ｓ１２０４で、検証に必要なデータを取得する。ここで検証に必要なデータとは、Ｎｏ．２の署名の情報が残っている署名履歴３１３と、新聞公開署名記録１２１４（公開機関のＮｏ．１０５の署名記録）と、公開機関のＮｏ．１０５の署名記録が新聞公開された時に、ユーザによるＮｏ．７の公開署名記録の公開依頼に対して、公開機関側装置から送信された公開機関のＮｏ．１０１～Ｎｏ．１０５の署名履歴２１３である。新聞公開署名記録は、検証に利用する署名履歴２１３中に含まれていなければならない。検証に利用する新聞公開署名記録が公開機関側装置から送られた署名履歴に含まれていない場合は、必要な公開機関の署名履歴２１３を、検証するユーザが要請して取得しても良い。

【００９０】

Ｓ１２０５で、連鎖の検証を行う。連鎖の検証は、以下のステップにより行う。

【００９１】

Ｓ１２０６で、新聞公開署名記録（Ｎｏ．１０５）１２１４が、公開機関の署名履歴２１３中のＮｏ．１０５の署名記録と一致するかどうか検証する。

【００９２】

Ｓ１２０７で、新聞公開された公開機関のＮｏ．１０５の署名記録から、ユーザのＮｏ．７の公開署名記録を受信した時に作成した公開機関の署名記録（Ｎｏ．１０１の署名記録）まで連鎖が繋がっているか検証する。連鎖検証の際には、署名記録中に残された前回署名記録のハッシュ値６０７と、その１つ前の署名記録のハッシュ値とを比較し、一致すれば前後の連鎖は繋がっており、一致しなければ連鎖は途切れていると判断する。

【００９３】

Ｓ１２０８で、ユーザの公開署名記録（Ｎｏ．７の署名記録）が添付された公開依頼書を受信した時に作成された公開機関側装置の署名履歴２１３中のＮｏ．１０１の署名記録に含まれる「受信した公開署名記録情報６０９」の内容「署名番号と公開署名記録（Ｎｏ．７の署名記録）のハッシュ値を結合したもの」と、ユーザ側装置の署名履歴３１３中のＮｏ．７の署名記録に含まれる項目６０９の内容「署名番号とＮｏ．７の署名記録のハッシュ値を結合したもの」が一致するか検証する。

【００９４】

Ｓ１２０９で、ユーザ側装置の署名履歴３１３において、公開署名記録（Ｎｏ．７の署名記録）から検証対象署名の署名記録（Ｎｏ．２の署名記録）までの連鎖を検証する。連鎖検証の際には、署名記録中に残された「前回署名記録のハッシュ値４０４」と、その１つ

前の署名記録のハッシュ値とを比較し、一致すれば前後の連鎖は繋がっており、一致しなければ連鎖は途切れていると判断する。

【００９５】

以上、Ｓ１２０６からＳ１２０９まで全ての検証が成功すれば、連鎖の検証は成功であり、Ｓ１２０１、Ｓ１２０２、Ｓ１２０５の検証が全て成功すれば、検証対象署名の検証は成功である。

【００９６】

上記では、公開機関側装置の署名記録を新聞公開することによって、公開機関の不正を防ぎ、確実に署名の正当性を検証する例を示した。公開機関の署名履歴を使わず、以下に示すような別の方法を用いても良い。

【００９７】

公開機関側装置は、ある一定の期間に複数のユーザ側装置から受信した公開署名記録を結合し、そのハッシュ値をとる。このハッシュ値を公開用データとして新聞などのメディアを利用して公開することによって、公開機関の不正防止と、各ユーザが公開を依頼した公開署名記録の完全性が保証される。例えば、この公開データが公開された時に、別の検査機関が、公開機関によってＷｅｂなどに公開されているユーザの公開署名記録を利用して、公開データが正しいかどうか検証することによって、その署名の正当性を証明することもできる。

【００９８】

具体的な手順は以下の通りである。図１２において、公開機関側装置１０４の記憶装置２０２にはユーザＡ～Ｅのユーザ側装置から送られてきた公開署名記録を保存する。受信した公開署名記録は、Ｗｅｂなどに公開する。Ｗｅｂに公開した時に、公開機関がＷｅｂ公開通知書５０７をユーザに送ると、ユーザはＷｅｂ公開されたことを確認することができる。公開機関は、記憶装置２０２に保存された公開署名記録を利用して、定期的に新聞公開５０４を行う。日時ｔにおいて、まずその時点で各ユーザが公開機関に公開している最新の公開署名記録１３０１～１３０５からなるデータを、たとえば結合により作成する。この作成したデータにハッシュ関数を適用してハッシュ値を求め、そのハッシュ値を新聞公開用データとして新聞に公開する。

【００９９】

一定時間経過後の日時ｔ＋１に同様に、公開署名記録１３０６～１３１０に基づくハッシュ値を求め、日時ｔ＋１での新聞公開用データとして新聞に公開する。

【０１００】

上記のような公開データの作成と公開を、適当な時期に、または定期的に行い、新聞公開用データの作成に利用した公開署名記録を作成したユーザ側装置に、新聞公開通知書５０８を送信する。

【０１０１】

各ユーザ側装置は、公開された新聞公開用データと、Ｗｅｂなどに公開されている公開署名記録とを比較することによって、公開署名記録の改竄の有無を調べることができる。公開されている各ユーザの公開署名記録が一つでも改竄されていれば、新聞公開用データと、Ｗｅｂに公開されている公開署名記録に基づくハッシュ値とが一致しなくなり、改竄が発覚する。

【０１０２】

上述した公開機関の不正の有無は、各ユーザ側装置ではなく、上述していない他の検査機関の装置において検査してもよい。

【０１０３】

公開機関側装置１０４がある一定の期間内に受信した公開署名記録からなるデータに基づいて作成され、公開された新聞公開用データと、ユーザの公開署名記録と署名履歴を用いて、当該ユーザの署名を検証する方法を以下に示す。検証前に、予め、検査機関の報告などを調べて、公開機関によるＷｅｂ公開に不正が無いかどうか確認しておく。

【０１０４】

例えば、図１３において、Ｎｏ．２の署名付き文書１４０５を検証する時、Ｓ１４０１で、検証対象文書と検証対象署名に対して公開鍵を用いて通常の署名検証を行い、Ｓ１４０２で、検証対象署名と署名履歴３１３のＮｏ．２の署名記録の中に検証対象署名があるかどうか検証する。

【０１０５】

Ｓ１４０３で、Ｗｅｂ公開されている公開署名記録と署名履歴３１３とに含まれる同じ署名番号の署名記録（本例では、Ｎｏ．７の署名記録）が一致するか検証する。

【０１０６】

Ｓ１４０４で、ユーザの署名履歴３１３について、Ｓ１４０３で検証した公開署名記録（Ｗｅｂ公開された公開署名記録と同じ番号の署名記録）から検証対象署名のＮｏ．２の署名記録まで連鎖が繋がっているか検証する。連鎖の検証は上記実施例と同様に行う。

【０１０７】

Ｓ１４０１～Ｓ１４０４の検証が全て成功すれば、検証対象署名の検証は成功である。

【０１０８】

【発明の効果】

本発明による、公開機関がユーザ側装置の署名記録の公開を代行する仕組みにより、より多くのユーザが自身の署名の正当性を証明できるようになる。

【図面の簡単な説明】

【図１】本発明の第１実施形態が適用されたシステムの概略図である。

【図２】本公開システムにおける公開機関装置の構成図である。

【図３】本公開システムにおけるユーザ側装置の構成図である。

【図４】ヒステリシス署名技術の概略図である。

【図５】ユーザと公開機関の間でやり取りされる情報を表した図である。

【図６】署名履歴ファイルに格納されるデータの構成、また、ユーザ情報ファイルに格納されるデータの構成を説明するための図である。

【図７】公開システムの受信プログラムの処理内容を説明するためのフロー図である。

【図８】公開システムの送信プログラムの処理内容を説明するためのフロー図である。

【図９】公開システムの新聞公開プログラムの処理内容を説明するためのフロー図である。

【図１０】公開システムの履歴送信プログラムの処理内容を説明するためのフロー図である。

【図１１】ユーザが、新聞等に公開された公開機関の署名記録、署名履歴送信プログラムによって公開機関より送られてきた公開機関の署名履歴、各ユーザの公開署名記録、各ユーザの署名履歴を用いて、署名を検証する方法を説明した図である。

【図１２】各ユーザから受信した情報を用いて公開用データを作成し、新聞公開する方法を説明した図である。

【図１３】公開機関が、ある一定の期間内に受信した全ての公開署名記録を結合し、そのハッシュ値を公開用データとして新聞公開した場合の、ユーザが、各ユーザの公開署名記録、各ユーザの署名履歴を用いて、署名を検証する方法を説明した図である。

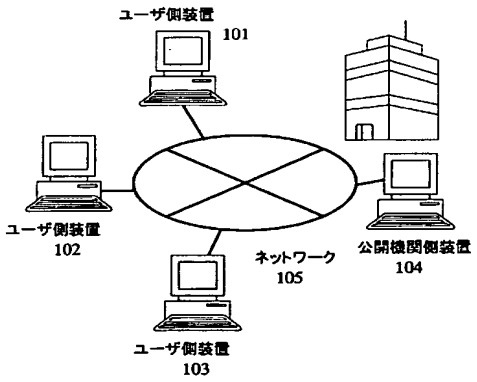
【符号の説明】

１０１～１０３：ユーザ側装置、１０４：公開機関側装置、１０５：ネットワーク、２０１：ＣＰＵ、２０２：記憶装置、２０３：インタフェース、２０４：通信装置、２０５：入力装置、２０６：表示装置、２０７：Ｗｅｂサーバ、２０８：公開依頼書受信プログラム、２０９：公開通知書送信プログラム、２１０：新聞公開プログラム、２１１：履歴送信プログラム、２１２：ユーザ管理プログラム、２１３：署名履歴ファイル、２１４：ユーザ情報ファイル、２１５：公開署名記録保存ファイル、３０１：ＣＰＵ、３０２：記憶装置、３０３：インタフェース、３０４：通信装置、３０５：入力装置、３０６：表示装置、３０７：送信プログラム、３０８：受信プログラム、３０９：文書検証プログラム、３１０：公開依頼書送信プログラム、３１１：履歴送信プログラム、３１２：履歴受信プログラム、３１３：署名履歴ファイル、３１４：ユーザ情報ファイル、３１５：他ユーザ

署名履歴保存ファイル、４０１：項目（「識別番号」）、４０２：項目（「署名番号」）、４０３：項目（「種別」）、４０４：項目（「前回署名記録のハッシュ値」）、４０５：項目（「文書のハッシュ値」）、４０６：項目（「署名または受信署名記録情報」）、４０７：送信文書、４０８、４１０：署名、４０９：受信文書、４１２～４１５：署名記録、５０６：公開依頼書、５０７：Ｗｅｂ公開通知書、５０８：新聞公開通知書、６０１～６０３：レコード、６０４：項目（「識別番号」）、６０５：項目（「署名番号」）、６０６：項目（「種別」）、６０７：項目（「前回署名記録のハッシュ値」）、６０８：項目（「文書のハッシュ値」）、６０９：項目（「署名または受信した公開署名記録情報」）、６１０～６１６：レコード、６１７：項目（「署名番号」）、６１８：項目（「種別」）、６１９：項目（「相手情報」）、６２０：項目（「受信署名番号」）、６２１：項目（「公開署名記録」）、６２２：項目（「日時」）、１２１０：検証対象文書、１２１４：新聞公開署名記録、１３０１～１３０５：日時ｔで各ユーザが公開機関に公開している最新の公開署名記録、１３０６～１３１０：日時ｔ＋１で各ユーザが公開機関に公開している最新の公開署名記録、１４０５：検証対象文書、１４０６：ユーザの署名履歴。

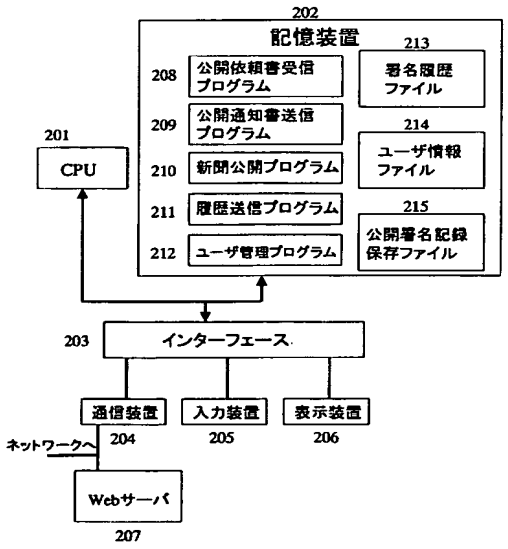
【図１】

図１



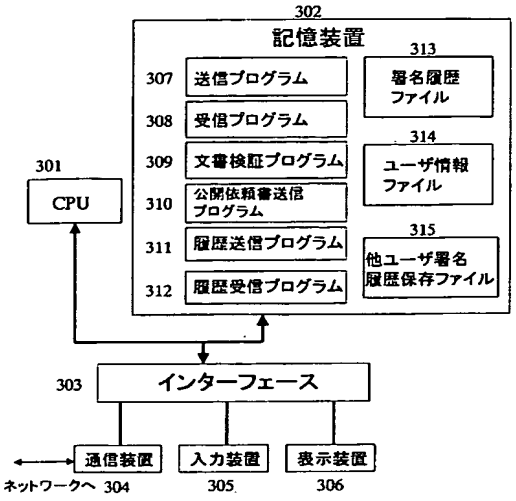
【図２】

図２



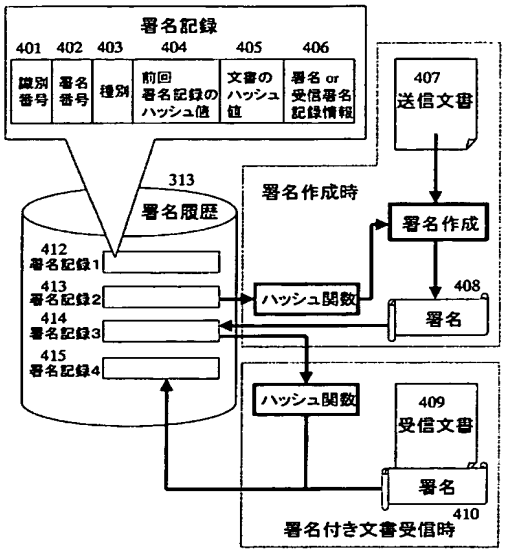
【図３】

図３



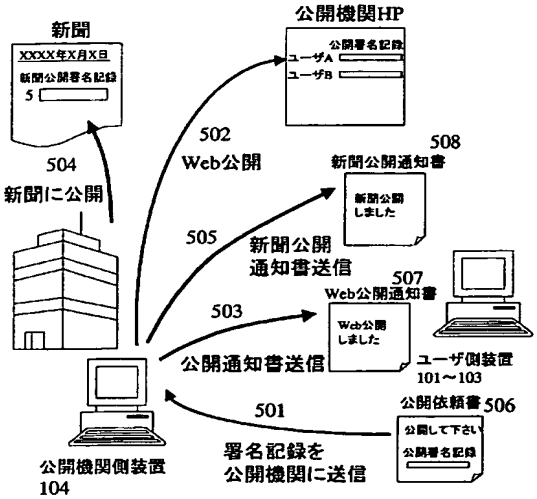
【図４】

図４



【図５】

図５



【図６】

図６

署名履歴ファイル

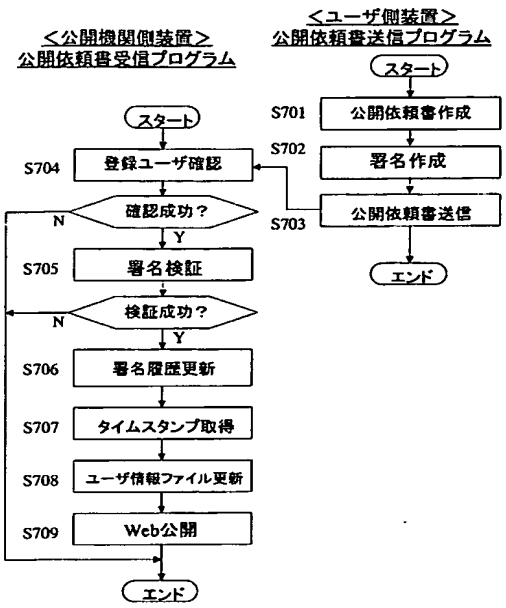
	604 識別番号	605 署名番号	606 種別	607 前回署名記録のハッシュ値	608 文書のハッシュ値	609 署名 or 受信した公開署名記録情報
601	Ver.1.0	1	受信	$H(S_0)$	—	$31 \| H(S_{31})$
602	Ver.1.0	2	送信	$H(S_1)$	$H(M_2)$	$Sign(2 \| H(S_1) \| H(M_2))$
603	Ver.1.0	3	受信	$H(S_2)$	—	$15 \| H(S_{15})$

ユーザ情報ファイル

	617 署名番号	618 種別	619 相手情報	620 受信署名番号	621 公開署名記録	622 日時
610	0	新聞公開	新聞	—	—	
611	1	受信	ユーザA@XXX.co.jp	32	S_{31}	2002.1017.0816
612	2	送信	ユーザA@XXX.co.jp	—	—	—
613	3	受信	ユーザB@XXX.co.jp	16	S_{15}	2002.1019.1550
614	4	送信	ユーザB@XXX.co.jp	—	—	—
615	5	新聞公開	新聞	—	S_4	2002.1020
615	6	履歴送信	ユーザA@XXX.co.jp	—	—	—

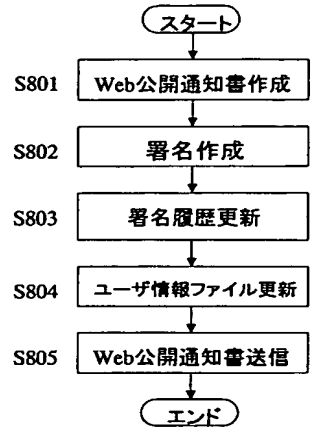
【図７】

図７



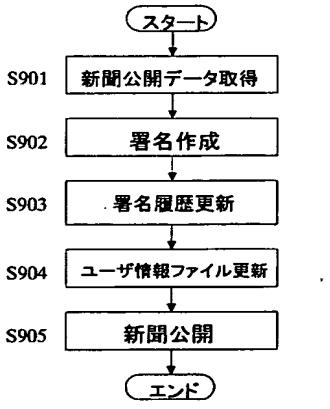
【図８】

図８



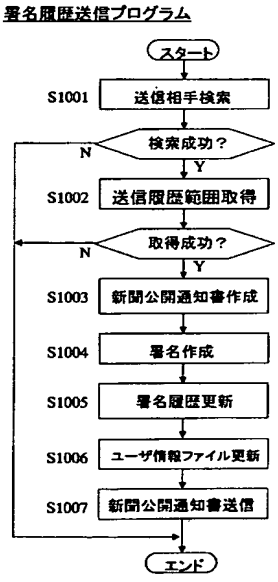
【図９】

図９



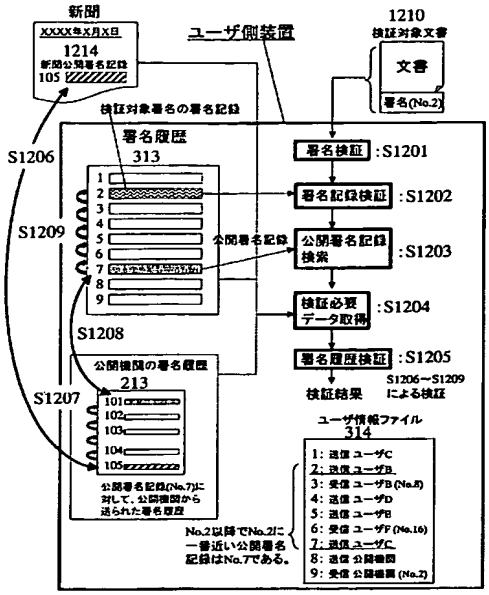
【図１０】

図１０



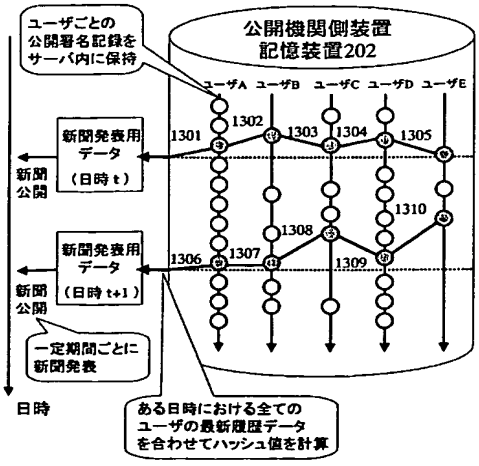
【図１１】

図１１



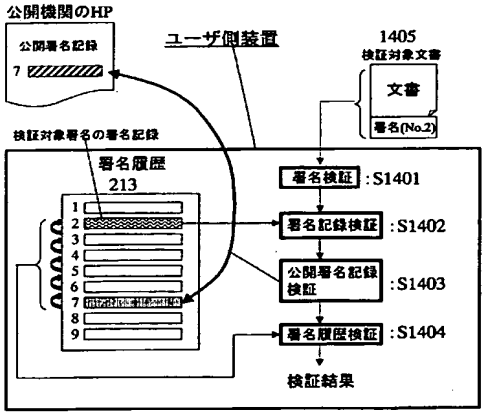
【図１２】

図１２



【図１３】

図１３



フロントページの続き

(72)発明者 伊藤 信治
神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所システム開発研究所内
(72)発明者 工藤 康明
東京都江東区新砂一丁目６番２７号 株式会社日立製作所公共システム事業部内
(72)発明者 別所 良治
東京都江東区新砂一丁目６番２７号 株式会社日立製作所公共システム事業部内

Fターム(参考) 5J104 AA09